

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT

INVENTOR(S) : James H. Moore
TITLE : METHOD FOR VERIFYING
CHRONOLOGICAL INTEGRITY OF
AN ELECTRONIC TIME STAMP
APPLICATION NO. : 09/468,157
FILED : December 21, 1999
CONFIRMATION NO. : 3291
EXAMINER : Kyung H. Shin
ART UNIT : 2143
LAST OFFICE ACTION : October 13, 2004
ATTORNEY DOCKET NO. : D99748
XERZ 2 00696

**TRANSMITTAL OF
APPEAL BRIEF UNDER 37 C.F.R. §1.192**

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant transmits herewith one (1) copy of APPEAL BRIEF UNDER 37 C.F.R. §1.192 for the above-reference patent application.

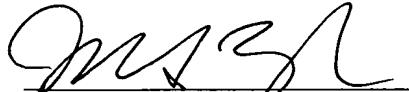
Applicant hereby petitions the Commissioner under 37 C.F.R. § 1.136(a) and request a two (2)-month extension of time up to and including at least February 13, 2005 to file this Appeal Brief. Fees in the amount of \$450.00 are included in our attached check.

The commissioner is authorized to charge Deposit Account
No. 24-0037 for the fee of \$330.

Respectfully submitted,

FAY, SHARPE, FAGAN,
MINNICH & MCKEE, LLP

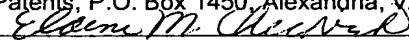
Date: 2/14/05



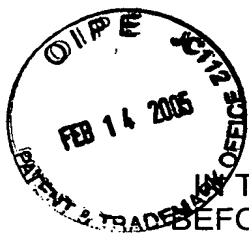
John S. Zanghi, Esq., Reg. No. 48,843
1100 Superior Avenue, Seventh Floor
Cleveland, Ohio 44114-2518
216.861.5582

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this Transmittal of Appeal Brief Under 37 C.F.R. §1.192 is being sent by the United States Postal Service as Express Mail procedure and is addressed to Mail Stop – Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. Express Mail No. EV 494957160 US


Elaine M. Checovich

Date: 2-14-05



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND
INTERFERENCES

In re the Application of: James H. Moore

Application No.: 09/468,157

Examiner: Kyung H. Shin

Filed: December 21, 1999

Docket No.: D99748
XERZ 2 00696

For: METHOD FOR VERIFYING CHRONOLOGICAL INTEGRITY OF AN
ELECTRONIC TIME STAMP

BRIEF ON APPEAL

Appeal from Group 2132

02/16/2005 MAHMED1 00000033 240037 09468157
01 FC:1402 500.00 DA

FAY, SHARPE, FAGAN, MINNICH & MCKEE, LLP
1100 Superior Avenue – Seventh Floor
Cleveland, Ohio 44114-2579 22320
Telephone: (216) 861-5582
Attorneys for Appellants

TABLE OF CONTENTS

	<u>Page</u>
<u>TABLE OF CONTENTS</u>	i
<u>TABLE OF AUTHORITIES</u>	ii
I. <u>REAL PARTY IN INTEREST</u>	1
II. <u>RELATED APPEALS AND INTERFERENCES</u>	1
III. <u>STATUS OF CLAIMS</u>	1
IV. <u>STATUS OF AMENDMENTS</u>	1
V. <u>SUMMARY OF CLAIMED SUBJECT MATTER</u>	1
VI. <u>GROUND OF REJECTION TO BE REVIEWED ON APPEAL</u>	3
VII. <u>ARGUMENT</u>	5
A. Claim 1 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle	5
B. Claim 3 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle	8
C. Claim 4 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle	9
D. Claim 5 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle and Labozzeta	10
E. Claim 6 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle	11
F. Claim 7 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle	12
VIII. <u>CONCLUSION</u>	13
<u>CLAIMS APPENDIX</u>	A-1
<u>EVIDENCE APPENDIX</u>	B-1
<u>RELATED PROCEEDINGS APPENDIX</u>	C-1

TABLE OF AUTHORITIES

Cases

<i>Grain Processing Corp. v. American Maize-Prods. Co.</i> , 840 F.2d 902 (Fed. Cir. 1988)	7
<i>In re Clay</i> , 966 F.2d 656 (Fed. Cir. 1992)	11
<i>In re Gordon</i> , 733 F.2d 900 (Fed. Cir. 1984)	7
<i>In re Laskowski</i> , 871 F.2d 115 (Fed. Cir. 1989)	7
<i>In re Napier</i> , 55 F.3d 610 (Fed. Cir. 1995)	7
<i>In re Rouffet</i> , 149 F.3d 1350 (Fed. Cir. 1998)	7
<i>McGinley v. Franklin Sports, Inc.</i> , 262 F.3d 1339 (Fed. Cir. 2001)	8
<i>Tec Air, Inc. v. Denso Manufacturing Michigan Inc.</i> , 192 F.3d 1353 (Fed. Cir. 1999)	8

Statutes

35 U.S.C. §103(a)	3, 4
-------------------	------

I. REAL PARTY IN INTEREST

The real party in interest for this appeal and the present application is Xerox Corporation, by way of an Assignment recorded in the U.S. Patent and Trademark Office at Reel 10478, Frame 463-464.

II. RELATED APPEALS AND INTERFERENCES

There are no prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1 and 3-7 stand rejected and have been appealed. In addition, claim 1 has been currently amended to correct a minor informality in the preamble, which was noted in the Final Office Action mailed April 14, 2004.

Claim 2 has been cancelled.

IV. STATUS OF AMENDMENTS

Subsequent to the Final Action mailed on April 14, 2004, Applicant submitted an Amendment After Final on July 14, 2004. By an Advisory Action dated October 6, 2004, the Examiner indicated that the requested claim amendments had been entered but did not place the application in condition for allowance. Claim 1 has been currently amended to correct a minor informality in the preamble, as noted in the Final Office Action mailed April 14, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claims do not stand or fall together. Each claim is to be considered by the Board in view of the arguments and comments submitted herein.

The subject matter of independent claim 1 is directed to a method for securing the integrity of files prior to archiving of the files and involves an exchange between a client and a Time Source Provider. The method comprises the client generating a Public and a Private Key pair that is organizationally associated (page 6, lines 2-3) and the Time Source Provider generating a public and private key pair for use in transactions with the client (page 6, lines 5-7). The client then generates attributes of the files to be archived, where the attributes include file sizes and cryptographic signatures (page 6, lines 8-9). The client's files are encrypted utilizing the client's Public Key (page 6, lines 9-10), and the encrypted files and the client's Public Key signature are to the Time Source Provider (page 6, lines 16-18). The Time Source Provider decrypts the encrypted data and file attributes with the Time Source Provider's Private Key and then with the client's Public Key (page 6, lines 21-23). The Time Source Provider then creates a TimeMap containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client (page 6, line 27 to page 7, line 14). The Time Source Provider returns the client's data along with the time map and session key signature and provides the encrypted client data back to the client (page 7, lines 21-23). The client archives the original files, file attributes and the time map from the Time Source Provider (page 7, lines 27-29).

Claim 3 adds the feature of the client providing multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map (page 6, line 29, to page 7, line 5).

Claim 4 adds the feature of exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction (page 7, lines 15-21).

Claim 5 adds the application of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures (page 4, lines 7-11).

Claim 6 adds the steps of the client producing the archived files, file attributes and time map, with the Time Source Provider retrieving the time map and session key, regenerating the time map, encrypting the time map with the session key and comparing the regenerated time map to the time map (page 8, lines 1-8).

Claim 7 adds the steps of establishing a clear channel transaction interval and pattern, the client encrypting the clear channel transaction using the client's Public and Private key pair, sending the clear channel transaction to the Time Source Provider, and triggering an alarm if the clear channel transaction is not received by the Time Source Provider (page 9, lines 21-31, to page 10, lines 1-2).

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review:

Claim 1 was rejected as having been obvious under 35 U.S.C. §103(a) over Haber, et al (U.S. Patent No. 5,136,647) in view of Romney, et al. (U.S. Patent No. 6,085,322) and further in view of Doyle (U.S. Patent No. 6,381,696).

Claim 3 was rejected as having been obvious under 35 U.S.C. §103(a) over Haber in view of Romney and further in view of Doyle.

Claim 4 was rejected as having been obvious under 35 U.S.C. §103(a) over Haber in view of Romney and further in view of Doyle.

Claim 5 was rejected as having been obvious under 35 U.S.C. §103(a) over Haber in view of Romney and further in view of Doyle and further in view of Labozzetta (U.S. Patent No. 6,107,269).

Claim 6 was rejected as having been obvious under 35 U.S.C. §103(a) over Haber in view of Romney and further in view of Doyle.

Claim 7 was rejected as having been obvious under 35 U.S.C. §103(a) over Haber in view of Romney and further in view of Doyle.

VII. ARGUMENT

A. Claim 1 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle

The present application teaches an improved method for securing the integrity of files prior to archiving and involves an exchange between a client and a Time Source Provider, which, in this case, is a trusted third party. In particular, as defined in claim 1: (a) both the Client and the Time Source Provider must have the ability to generate Public and Private Key pairs, (b) the encrypted data and file attributes along with the client's Public Key are to be transmitted to the Time Source Provider, (c) the Time Source Provider decrypts the encrypted data and file attributes with the Time Source Provider's Private Key and with the client's Public Key, and (d) the client's Public and Private Key pair is organizationally associated. If the key pair is reserved for archiving, then the risk of exposure and compromising is decreased. None of these concepts are fairly taught or suggested by the references cited by the Examiner.

Haber relates to a method of time-stamping a digital document and authenticating the document by means of the agency's public key to reveal the receipt. The receipt comprises the hash of the alleged document along with the time seal that only the agency could have signed into the certificate. As noted by the Examiner, however, Haber does not teach or suggest the steps of generating Private and Public Key pairs for the client and the Time Source Provider or using the Key pairs for encrypting and decrypting the data and file attributes.

While Romney arguably discloses the step of the client generating a public/private key pair, Romney does not disclose the additional steps of the Time Source Provider generating *its own public/private key pair*, whereby the two sets of key pairs are used to encrypt and decrypt the data and file attributes (see FIG. 2 in Romney).

Doyle relates to the digital time stamping of data, without the need for subsequent third party verification, by the chaining of key pairs, the key pairs being generated for particular time intervals. Doyle, does not, however, teach or suggest the concepts of the present application. In column 5, lines 34-39, Doyle discloses:

In step 2010 a key pair is generated. As is known in the art, the key pair includes a public key and a private key. According to an embodiment of the present invention, a key pair is generated for each time interval utilized by the system implementing the time stamping method. The implementing system can include, for example, a conventional general purpose computer, such as a microprocessor based personal computer or server. In an embodiment of the present invention, the method is implemented in software that executes on a client-server computer system architecture. The time interval can be any defined period, e.g., every second, 10 seconds, minute or 10 minutes. The current time interval is referred to as t_n and the next time interval is referred to as t_{n+1} . For the purposes of time stamping documents, accuracy to the minute may be sufficient for subsequent authentication purposes.

Nonetheless, Doyle¹ fails to teach or suggest that the public and private key pair is "organizationally associated" as provided in claim 1. That is, Doyle does not disclose that each key pair is to be associated with a specific organization/corporate unit, or individual. (See page 6, lines 2-3 of the present application.) Rather, in column 8, lines 36-50, Doyle summarizes that:

key pairs are generated *for particular time intervals* and time stamp requests are automatically carried out using the private key for the time interval, the private key being destroyed after the time interval. In another embodiment of the present invention, the private key of a prior time interval is used to sign the public key for a subsequent time interval before the private key of the prior time interval is destroyed. In this embodiment of the present invention, every time interval has its own key pair for which the private key is destroyed after signing the public key for the next time interval. According to the present invention, key pairs do not have to be continuously generated every time interval, but can be pre-generated and selected from a queue for each time interval that a time stamp request is received. (Emphasis added.)

¹ In the Final Office Action the Examiner cited Romney in connection with original claim 2. However, it is believed that the Examiner intended to cite Doyle.

Generating key pairs for “particular time intervals” is not the same as generating key pairs that are “organizationally associated.”

Further, there is no motivation to modify Haber to generate a Public and Private key pair and signature the encrypted data as taught in Romney or in Doyle. Applicant asserts that it could only be through the use of impermissible hindsight that the Examiner could reach a conclusion of obviousness. The Examiner has used Applicant's disclosure as a guide through the references, combining the references in just the right order so as to arrive at Applicant's claimed invention. This is an impermissible approach. See *Grain Processing Corp. v. American Maize-Prods. Co.*, 840 F.2d 902, 907 (Fed. Cir. 1988). Indeed, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure. See *In re Laskowski*, 871 F.2d 115, 117 (Fed. Cir. 1989) (“[T]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification”) (quoting *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984)). Indeed, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner cited. *In re Rouffet*, 149 F.3d 1350 (Fed. Cir. 1998). See also *In re Napier*, 55 F.3d 610, 631 (Fed. Cir. 1995) (“Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination.”).

Still further, there is no suggestion to combine the teachings of Haber with those of Romney and Doyle because Haber teaches away from its combination with Romney and Doyle. For example, Romney teaches that the “two message digests X and Y will be identical only if the private key used by the authenticator to decrypt the

digital signature are a valid public-private key pair.” (Romney, col. 5, lines 19-25.) Likewise, Doyle teaches generating a public and private key pair. (Doyle, col. 5, lines 33-39.) On the other hand, as noted in the background section, it is an objective of Haber to develop a reliable system of time-stamping documents *without the use of a “private key.”* (Haber, col. 1, lines 63, to col. 2, lines 1-30.) Therefore, the teachings of Romney and Doyle would teach away from the object of Haber’s invention, thereby not providing any motivation to combine the aforementioned teachings. See *Tec Air, Inc. v. Denso Manufacturing Michigan Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999):

There is no suggestion to combine . . . if a reference teaches away from its combination with another source. . . . “A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant . . . [or] if it suggests that the line of development flowing from the reference’s disclosure is unlikely to be productive of the result sought by the applicant.”

As recently noted by the Federal Circuit, references that teach away from the claimed invention cannot serve to create a *prima facie* case of obviousness. See *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339 (Fed. Cir. 2001). That is the precise situation with the attempt to combine Haber with Romney and Doyle. As a result, the rejection of claim 1 over the combination of Haber with Romney and Doyle fails. Claim 1 is patentable over the art of record.

B. Claim 3 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle

Claim 3 depends from claim 1 and adds that the client provides multiple encryption of files, generates the signature of the file at each step, and provides all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map.

The preceding arguments in support of claim 1 apply as well to claim 3 of the present application. And, as noted by the Examiner, Haber does not teach the claimed features. As such, the Examiner claims that Doyle teaches the method of claim 3, citing col. 8, lines 56 and 65. Once again, however, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 3 as being unpatentable over Haber in view of Romney and further in view of Doyle is improper and must be reversed.

C. Claim 4 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View of Doyle

Claim 4 depends from claim 1 and adds the feature of exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction. The session key is typically a symmetric key such as DES because they are often much faster than Public Key/Private Key cryptography (see page 7, lines 17-19, of the present application). The session key is never shared with the client but is itself encrypted, and transmitted to a secured location along with the time map itself (see page 7, lines 5-7, of the present application).

The preceding arguments in support of claim 1 apply as well to claim 4 of the present application. And, as noted by the Examiner, Haber does not teach the use of a session key in generating the signature of the encrypted files between the client and the Time Source Provider for securing the exchange. As such, the Examiner claims that Doyle teaches a "session key," citing col. 9, lines 19-20. However, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 4 as being unpatentable over Haber in view of Romney and further in view of Doyle is improper and must be reversed.

D. Claim 5 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Doyle and Labozzeta

Claim 5 depends from claim 1 and further includes the "application of multiple or differing error correcting codes to the representation of time, the time source calibration data, the file attributes and the encryption key signatures," is separately patentable in view of the cited art. The preceding arguments in support of claim 1 apply as well to claim 5 of the present application.

As noted by the Examiner, neither Haber nor Doyle teaches the additional features of claim 5. Another cited reference, Labozzetta, relates to a device used in monopulse radar systems for correcting the differential error contained in the raw Off-Boresight Angle value obtained in such systems, especially when used for azimuth tracking, *i.e.*, it is a differential error correction device. As disclosed in Labozzetta in column 4, lines 5-20:

The statistical averaging and linearization performed in the feedback loop 22 substantially eliminates deterministic errors commonly found in systems used for differential error correction in monopulse receivers known presently in the art, an example of which is shown in FIG. 2. Such deterministic errors are commonly caused by variations of system tolerances and the effects of those tolerances on the antenna construction and design, as well as periodic time variations and thermal variations of the system, which could occur and produce errors in the same direction of the angular origin of the received radar signals. These deterministic errors, which produce inaccurate OBA detection in currently known differential error correction systems, are substantially eliminated through the use of the inventive feedback loop previously described.

Labozzetta, however, does not in any way teach or suggest *applying multiple or differing error correcting codes to the representation of time, the time source calibration data, the file attributes and the encryption key signatures.*

Moreover, Labozzetta relates to monopulse radar systems and error correction and does not teach the encryption of data. As such, Labozzetta constitutes nonanalogous art. For purposes of evaluating the obviousness of claimed subject matter, one must make certain that a particular reference relied upon constitutes "analogous art." *In re Clay*, 966 F.2d 656, 658-659 (Fed. Cir. 1992).

Due to the above-discussed non-obviousness of the proposed combination and the nonanalogous nature of Labozzetta, the rejection of claim 5 as being unpatentable over Haber in view of Doyle and further in view of Labozzetta is improper and must be reversed.

E. Claim 6 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View of Doyle

Claim 6 depends from claim 4 and adds the steps of the client producing the archived files, file attributes and time map, the Time Source Provider retrieving the time map and session key, the Time Source Provider regenerating the time map, the Time Source Provider encrypting the time map with the session key, and comparing the regenerated time map to the time map. The preceding arguments in support of claims 1 and 4 apply as well to claim 6 of the present application.

Claim 6 relates to a request for legal verification of authenticity and/or the time of archival of files, whereby the client would only have to produce the archive file and any encryption keys used by the client. (See page 8, lines 1-3, of the present application.) The originality of the time and time map may be readily verified by the method of claim 6. (See page 8, lines 6-8, of the present application.)

As noted by the Examiner, Haber fails to disclose the additional features of claim 6. As such, the Examiner claims that Romney teaches the method of claim 6. As disclosed in col. 7, lines 34-37, of Romney, the electronic document and the public/private key pair may be sent to the authenticator by electronic means. As

noted in col. 7, lines 42-47, the authenticator may, for example, take biometric readings of the client for identification. However, there is no mention of a "session key," as provided in claim 6.

Moreover, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure, aside from a general comment that one would be motivated to combine Haber and Romney to establish the authenticity of an electronic document.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 6 as being unpatentable over Haber in view of Romney and further in view of Doyle is improper and must be reversed.

F. Claim 7 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View of Doyle

Claim 7 depends from claim 1 and adds the steps of establishing a clear channel transaction interval and pattern, the client encrypting the clear channel transaction using the client's Public and Private key pair, sending the clear channel transaction to the Time Source Provider, and triggering an alarm if the clear channel transaction is not received by the Time Source Provider.

The preceding arguments in support of claim 1 apply as well to claim 7 of the present application. And, as noted by the Examiner, Haber does not teach the claimed features. As such, the Examiner claims that Doyle and Romney teach the method of claim 7. In particular, the Examiner cited col. 7, lines 42-45, in support of the argument that Doyle teaches the triggering of an alarm if the clear channel transaction is not received by the Time Source Provider. However, there is no specific disclosure of the triggering of an alarm in Doyle. Even so, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying Haber to arrive at Applicant's disclosure.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 7 as being unpatentable over Haber in view of Romney and further in view of Doyle is improper and must be reversed.

VIII. CONCLUSION

For all of the reasons discussed above, it is respectfully submitted that the rejections are in error and that each of the pending claims 1 and 3-7 patentably distinguish over the cited art and are in condition for allowance. For all of the above reasons, Appellants respectfully request this Honorable Board to reverse the rejections of claims 1 and 3-7.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read 'J. S. Zanghi', written in a cursive style.

John S. Zanghi
Registration No. 48,843

JSZ:emc

FAY, SHARPE, FAGAN, MINNICH & MCKEE, LLP
1100 Superior Avenue – Seventh Floor
Cleveland, Ohio 44114-2579
Telephone: (216) 861-5582

Filed: February 14, 2005

CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL:

1. (Currently Amended) A method for securing the integrity of files prior to archiving of said files, involving an exchange between a client and a Time Source Provider (~~a trusted third party~~) said method comprising the steps of:

the client generating a Public and a Private Key pair that is organizationally associated;

the Time Source Provider generating a public and private key pair for use in transactions with the client;

the client generating attributes of the to be archived files, attributes includes file sizes and cryptographic signatures;

encrypting the client's files utilizing the client's Public Key;

transmitting said encrypted data and file attributes and the client's Public Key signature to said Time Source Provider;

the Time Source Provider decrypting said encrypted data and file attributes with the Time Source Provider's Private Key and then with the client's Public Key;

the Time Source Provider creating a TimeMap containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client;

the Time Source Provider returns the client's data along with the time map and session key signature;

the Time Source Provider providing said encrypted client data back to the client; and

the client archives the original files, file attributes and the time map from said Time Source Provider.

2. (Canceled)

3. (Original) A method as in claim 1, where the client provides multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map.

4. (Original) A method as in claim 1, further comprising the step of where a session key is exchanged between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction.

5. (Original) A method as in claim 1 for application of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures.

6. (Previously Presented) A method as in claim 4, further comprising the steps of:

- the client producing said archived files, file attributes and time map;
- the Time Source Provider retrieving said time map and session key;
- the Time Source Provider regenerating said time map;
- the Time Source Provider encrypting said time map with said session key;

and,

- comparing said regenerated time map to said time map.

7. (Previously Presented) A method as in claim 1, further comprising the steps of:

- establishing a clear channel transaction interval and pattern;
- the client encrypting said clear channel transaction using the client's Public and Private key pair;
- sending said clear channel transaction to the Time Source Provider;
- triggering an alarm if said clear channel transaction is not received by the Time Source Provider.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE